

ABSTRACT

A method for generating electronic keys from two integer numbers a , b , includes the step of verifying that the numbers are prime relative to each other. This verification step comprises the operations of calculating the modular exponentiation $a^{\lambda(b)} \bmod b$, where λ is the Carmichael function, verifying that this modular exponentiation is equal to 1, storing the pair a , b when equality is verified, and reiterating the procedure with another pair when there is no verification. The invention applies to chip cards with a microprocessor having an arithmetic processor.

0931858-02601